УДК 65.012.8: 004.01
DOI: 10.31891/2307-5740-2020-286-5-4

БАКАЙ В. Й., ЗИМА В. М.
Хмельницький національний університет

НОВІ ВИКЛИКИ ТА ОСОБЛИВОСТІ СТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті розглянуто особливості створення системи інформаційної безпеки підприємства, що пов'язано з загальною комп'ютеризацією, інформатизацією та цифровізацією суспільства. З'ясовано, що значення інформаційної безпеки для підприємства зростає, з'являються нові загрози та виклики які мають бути оперативно вирішені. Окрім того у зв'язку з глобальною пандемією COVID-19 та особливостями віддаленої роботи перед підприємствами постали нові проблеми забезпечення своєї інформаційної безпеки. Відзначено нові виклики щодо зростання кіберзагроз та необхідність протидіяти їм, особливо у розрізі особливостей організації робочого процесу у часи пандемії. Для забезпечення розвитку підприємства за допомогою створення системи інформаційної безпеки запропоновано рекомендації на основі європейського досвіду захисту інформації компаній.

Ключові слова: інформація, економіка, інформаційна безпека підприємства, кіберзагрози, цифрові технології, інформатизація, хакерські атаки, система, підприємство.

BAKAY V., ZUMA V.
Khmelnytskyi National University

NEW CHALLENGES AND FEATURES OF SYSTEM CREATION OF INFORMATION SECURITY OF THE ENTERPRISE

The article considers the peculiarities of creating an information security system of the enterprise, which is associated with the general computerization, informatization and digitalization of society. It was found that the importance of information security for the company is growing, there are new threats and challenges that must be addressed quickly. In addition, due to the global COVID-19 pandemic and the peculiarities of remote work, companies have new challenges in ensuring their information security.

There are challenges to the growth of cyber threats and the need to counter them, especially in terms of the peculiarities of the organization of the work process during a pandemic. New challenges, as well as the peculiarities of the organization of work have drawn attention to information security, intensified rule-making activities in this area in the direction of strengthening control over information security, resolving disputes, strengthening countering cyber threats. In the new realities, when information technologies become global, information security is an integral part of the system of economic security of the enterprise and the economic security of the state as a whole.

To ensure the development of the enterprise through the creation of an information security system, recommendations based on the European experience of information protection of companies are proposed. Important steps are the actual support and control of the information security system of the enterprise. After all, in recent years there has been a rapid increase in threats related to information cybersecurity.

In addition, it is noted that reliable information security is a prerequisite for the transition to a model of sustainable development of an individual enterprise. To maintain a business, develop it and be competitive, it is necessary to create an effective information security system. The essence of the above gives grounds to assert that in the new realities, without proper protection of the information environment of the enterprise it is impossible to ensure its economic security.

Keywords: information, economy, information security of the enterprise, cyber threats, digital technologies, informatization, hacker attacks, system, enterprise.

Постановка проблеми. В сучасному суспільстві інформація стала одним із найважливіших стратегічних ресурсів, що забезпечує подальший розвиток підприємства. Саме тому інформація, як і решта ресурсів, потребує особливого захисту. У зв'язку з загальною комп'ютеризацією, інформатизацією та цифровізацією суспільства значення інформаційної безпеки для будь-якого суб'єкта господарювання зростає, з'являються нові загрози та виклики, які мають бути оперативно вирішені. Окрім того у зв'язку з глобальною пандемією COVID-19 та особливостями віддаленої роботи перед підприємствами постали нові проблеми забезпечення своєї інформаційної безпеки.

Проблема створення системи інформаційної безпеки набула особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем. У зв'язку зі зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, а також через реальність численних загроз проблема інформаційної безпеки вимагає до себе постійної і значної уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, призводять до необхідності комплексного підходу в ході вирішення цієї проблеми.

Аналіз останніх досліджень чи публікацій. Дослідженням інформаційної безпеки підприємств присвячені роботи таких вчених, як А. Абросимов, Ст. Адріанов, А. Афоничкин, С. Ашмаріна, А. Баутов, А. Голів, М. Давлетханов, А. Добрянин, Д. Дияконів, А. Еляков, А. Курило, В. Лазарєв, А. Макарова, Мешайкина, Р. Насакін, Р. Нижньогородців, А. Павлов, А. Пастюшков, П. Покровський, Ст. Савельєв, С. Симонов, Смирнов, Н. Столяров, В. Стрілець, Б. Татарських, Терехова, Ф. Удалов, В. Філіппова,

Р. Хайретдінов, Ст. Ярочкин та ін. Проте слід зазначити, що переважна більшість наявних робіт присвячені, насамперед, техніко-технологічним проблемам формування системи інформаційної безпеки, вирішувати які повинні спеціалісти в галузі інформаційних технологій. Сучасні дослідження в галузі інформаційної безпеки вкрай рідко порушують питання організаційного та економічного характеру. В сучасних дослідженнях розгляд цих факторів носить епізодичний, позасистемний характер, проте зростання масштабів проблеми та вагомість можливих негативних наслідків потребують проведення комплексних досліджень.

Виділення невирішених раніше частин загальної проблеми. Проте проблема створення системи інформаційної безпеки підприємства залишається недостатньо дослідженою. Це пов'язано з тим, що вчені, економісти тощо, значну увагу приділяють інформаційній безпеці держави, а також з відсутністю цілеспрямованого підходу до вирішення проблеми в цілому у тих вчених-економістів, які розглядали роль інформації в господарській діяльності підприємства.

Постановка завдання. Метою дослідження є обґрунтування теоретичних та методичних особливостей створення і розвитку системи інформаційної безпеки підприємства в нових реаліях.

Виклад основного матеріалу дослідження. У всіх економічно розвинутих країнах світу використовують переваги інформаційних технологій у підприємницькій діяльності. Це пояснюється тим, що традиційні методи не дозволяють зорієнтуватись в сучасному інформаційному потоці і проаналізувати динамічні процеси господарської діяльності підприємства. Швидше за все розвиваються технології, пов'язані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як електронна торгівля, електронний бізнес, електронний уряд, діджиталізація.

Широко відомою є фраза Натана Ротшильда: «Хто володіє інформацією – той володіє світом». Отримання раніше інших достовірної інформації про поразку Наполеона дозволило Ротшильдам провести безпрограшну гру з цінними паперами на Лондонській біржі. За одну ніч Ротшильд збагатився на 40 мільйонів фунтів стерлінгів та оволодів більшою часткою британської економіки. Тоді і народився його крилатий вислів. І він набирає більшої ваги для наших часів, які з початком переходу до постіндустріального виробництва, глобалізації та широкої комп'ютеризації суспільства прийнято називати інформаційною ерою.

Інформація – це загальнонаукове поняття, яке характеризує прямий і зворотній обмін відомостями між живими організмами, електронними приладами іншими системами, про навколишнє середовище, процеси, предмети та явища, які можуть набувати властивостей: релевантності, повноти, захищеності, своєчасності, достовірності, доступності та ергономічності.

У Законі України «Про інформацію» наведено звужене та формалізоване поняття терміну: під інформацією цей Закон розуміє «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі» [1]. Зрозуміло, що вибудовуючи аналогії ми можемо модифікувати поняття інформації пристосовуючи під необхідні умови, як обмін відомостями між підприємствами, між підприємством і державою, між державою і суспільством тощо, але слід розуміти, що сутність поняття не змінилася – ми переміщуємося між індивідуальним та більш високими структурними рівнями.

Підприємницька діяльність підприємства пов'язана з отриманням, переробкою, продукуванням та ліквідацією великої кількості інформації. В будь-якій сфері господарської діяльності робота з інформацією несе у собі певні ризики, нівелювати які покликана інформаційна безпека. Існує велика кількість визначень інформаційної безпеки, але щодо інформаційної безпеки підприємства найбільш доречні визначення, що були дані Сороківською О.А.: «Суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності» [2] та Хоффманом Л.Дж.: «Стан інформації, за якого забезпечується збереження визначених політикою безпеки властивостей інформації» [3]. Отже, інформація – це чинник, який може призвести до технологічних аварій, військових та політичних конфліктів, дезорганізації державного управління, фінансової системи.

Зрозумілим є те, що з розвитком інформатизації, яка спостерігається останніми роками у всьому світі, слід значну увагу приділяти саме інформаційній безпеці. Більша частина інтересів будь-якого підприємства визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні дії з боку зовнішніх або внутрішніх джерел можуть завдавати шкоду цим інтересам і становлять реальну загрозу для подальшої підприємницької діяльності самого підприємства. Не викликає сумніву і той факт, що між рівнем економічної безпеки і інформаційною складовою існує пряма взаємозалежність. Як показує практика, будь-яка акція, спрямована проти підприємства, розпочинається зі збору інформації, саме тому питання інформаційної безпеки давно ввійшли до головних пріоритетів практично всіх великих компаній. Усе більше керівників розуміють, наскільки небезпечною може бути інсайдерська інформація, системи обробки інформації і дії співробітників, які беруть участь у підприємницькій діяльності підприємства. Тому, зі зростанням науково-технічного прогресу зростає і необхідність вирішення проблеми інформаційної безпеки.

Дана проблема для українських підприємств полягає в тому, що в чинних нормативно-правових актах, які регулюють інформаційні відносини, поняття інформаційна безпека майже не застосовується, а в тих яких застосовується – не дається роз'яснення цього терміну. Частіше в нормативно-правових актах України розглядається захист інформації, що є важливою складовою інформаційної безпеки, але не відбиває

її у повній мірі. До того ж акцент зроблено на інформаційній безпеці держави і особи, а не на інформаційній безпеці підприємства. Незважаючи на недосконаліть законодавства, для успіху бізнесу, одна з першочергових задач є впровадження комплексних заходів з інформаційної безпеки.

В Україні законодавчо чітко не регламентовані вимоги до інформаційної безпеки підприємств, хоча роботи у цьому напрямку ведуться, і судячи з тенденцій нормотворення, ці вимоги будуть наближені до стандартів GDPR, поки ж інформаційна безпека підприємств кинута на відкуп самим підприємствам, окрім банківського сектору, діяльність якого регламентується НБУ «Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків».

Для підприємства необхідно затвердити внутрішнім документом свою політику інформаційної безпеки. При написанні політики інформаційної безпеки слід керуватися принципами простоти, чіткості, послідовності, відповідності принципам безпеки підприємства. Для цього необхідно зробити акцент на наступних пунктах:

1. Покращення обізнаності персоналу, адже необізнаний персонал є «слабкою ланкою» у інформаційній безпеці, тому варто інформувати персонал про актуальні загрози, способи захисту, протидії їм, проводити тренінги з безпеки інформації та даних, відпрацьовувати зв'язки з відділом безпеки та інструкції з забезпечення безпеки інформації.

2. Захист фізичних носіїв інформації та робочих пристроїв, встановлення регламентів входу в систему, проводити регулярне резервне копіювання файлів та діагностику.

3. Сегментування мережі та контроль користувачів, які намагаються увійти.

4. Співпраця з перевіреними постачальниками послуг.

5. Захист віддаленого доступу до мережі вашого підприємства. Цей пункт особливо актуальний у часи пандемії, коли більшість персоналу вимушена працювати віддалено, щоб забезпечити робочу мережу пристрій віддаленого співробітника має відповідати наступним вимогам:

– підключення через віртуальну приватну мережу (VPN);

– використання двофакторної аутентифікації під час входу в систему або підключення до VPN;

– отримання доступу за допомогою віртуальної машини як опції підключення за замовчуванням, якщо це можливо;

– використання комплексного рішення з безпеки для захисту від проникнення програм-вимагачів, шпигунських програм та інших видів загроз, а також запобігання фішинг-атакам [4].

Останніми кроками є власне підтримка і контроль системи інформаційної безпеки підприємства. Адже, в останні роки відбувається стрімке зростання загроз пов'язаних з інформаційною кібербезпекою. Так, за даними Форіншурер страхування, на протязі останнього десятиліття відбувається швидка еволюція кіберризиків, вони виявляють стійку тенденцію до просування у топ-рейтингу – на разі вони знаходяться на другому щаблі з коефіцієнтом 0,4. Це пов'язано з появою нових програм вимагачів – WannaCry, Operation Cloud Hopper та Petya, посиленням частоти, масовості і серйозності DdoS атак, появою «кібер-ураганів», еволюцією програм-шпигунів – як-то вірус-троян Guildma, які створили значну загрозу банківській і фінансовій сфері у країнах по всьому світі. Хакери намагаються впливати на функціонування бізнесу шляхом впливу на загальні елементи інтернет-інфраструктури від якої він залежний [5].

За даними РНБО в Україні у 2020 році було зафіксовано близько 1 млн кіберзагроз – серед яких фішинг, Ddos-атаки, Web-атаки, спроби мережевого сканування, мережеві атаки, поширення шкідливого програмного забезпечення і т.п [6]. Так, усвідомлюючи небезпеку в інтернет-просторі, ще у 2001 році у Будапешті була прийнята Конвенція Ради Європи про кіберзлочинність, яка була ратифікована півсотнею країн, в тому числі і країнами які не є учасниками Ради Європи – США, Канадою, Японією, Австралією. У 2003 році була прийнята резолюція Генасамблеї ООН, яка зазначала необхідність розвитку глобальної кіберкультури і у тому ж році була прийнята Женевська декларація. У 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security). У 2013 році була ухвалена стратегія кібербезпеки в рамках ЄС, метою якої є створення безпечного, надійного, відкритого, стійкого кіберпростору в Європі.

У 2016 році була ухвалена Директива ЄС 2016/1148 щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі (NIS Directive) і створена команда з реагування на комп'ютерні надзвичайні події – CSIRT (Computer Security Incident Team). CSIRT відповідає за:

– моніторинг та реагування на випадки кіберзагроз;

– надання аналізу ризиків та аналізу інцидентів та ситуаційної обізнаності;

– участь у мережі CSIRT;

– співпраця з приватним сектором;

– сприяння використанню стандартизованої практики для інцидентів та класифікації ризиків та інформації [7].

В Україні з 2009 року діє Урядова команда реагування на комп'ютерні надзвичайні події – CERT-UA, яка виконує аналогічні функції. А у 2015 році було створено кіберполіцію як інструмент реагування та протидії кіберзлочинам. У 2017 році відбулось оновлення стратегії кібербезпеки, а також видано пакет

законів з кібербезпеки, який суттєво посилив моніторинг кіберзагроз і відстежування кібератак у Європі. Масштабні порушення інформаційної безпеки у США і Європі у 2018 році знову привернули увагу до необхідності покращення засобів захисту. Тому, у травні 2018 року у Європі було впроваджено Генеральний регламент про захист даних, скорочено – GDPR, а в США в червні того ж року – California Consumer Privacy Act 2018, або CCPA, які суттєво посилили, а також уніфікували захист даних, а якщо казати про GDPR, то він встановив чіткі регламенти роботи з агентами не з ЄС, а також обмежив експорт даних з території ЄС.

В Україні діє свій аналог, який, тим не менш, не є тотожним вище перерахованим документам – Закон України «Про захист персональних даних» від 2010 року, з останньою редакцією у 2020 році, але компанії, які хочуть працювати у ЄС та США, або мають справу з даними їх резидентів мають дотримуватись GDPR, або CCPA. Дотримання норм викладених у цих документах – це також гарний шанс підприємствам продемонструвати іноземним контрагентам відповідальність у роботі з даними.

Висновки. На прикладі Європи можна побачити, що формування системи інформаційної безпеки – складний, довготривалий, багатофакторний та багатогранний процес. Становлення цієї системи в Європі проходило методично та цілеспрямовано, а також різнонаправлено, тобто у всіх сферах: суспільній, господарській та державній. В Україні ж цей процес відбувається не систематично, і нормотворча активність активізувалась у 2014 році, до того ж є великий перегин у сторону державної і суспільної інформаційної безпеки, а інформаційній безпеці підприємств – приділяється недостатньо уваги. Нові виклики 2019–2020 рр., а також особливості організації роботи привернули увагу до інформаційної безпеки, активізували нормотворчу діяльність у цій сфері у сторону посилення контролю за інформаційною безпекою, урегулюванням спірних моментів, посиленням протидії кіберзагрозам.

Таким чином, в нових реаліях, коли інформаційні технології набувають глобального характеру, інформаційна безпека є невід'ємним складником системи економічної безпеки підприємства й економічної безпеки держави загалом. В свою чергу, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку окремого підприємства. Щоб зберегти бізнес, його розвивати і бути конкурентоспроможним, необхідно створити ефективну систему інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в нових реаліях, без належного захисту інформаційного середовища підприємства неможливо забезпечити його економічну безпеку.

Література

1. Про інформацію [Електронний ресурс] : Закон України від 02.10.1992 № 2658-XII // Відомості Верховної Ради України. – 1992. – № 48. – ст. 651. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2657-12#Text.

2. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Вісник Хмельницького національного університету. Серія: Економічні науки. – 2010. – № 2. – Т. 2. – С. 32–35.

3. Хоффман Л.Дж. Современные методы защиты информации / Л. Дж. Хоффман ; пер. с англ. – М. : Сов. радио, 1980. – 57 с.

4. Нові виклики для інформаційної безпеки підприємства: як мінімізувати потенційні ризики [Електронний ресурс]. – Режим доступу : https://eset.ua/ua/blog/view/67/novyye-vyzovy-dlya-informatsionnoy-bezopasnosti-predpriyatiya-kak-minimizirovat-potentsialnyye-riski.

5. Барометр рисков. Allianz назвал глобальные риски компаний в 2018 году // Фориншурер страхование [Електронний ресурс]. – Режим доступу : https://forinsurer.com/news/18/01/26/35755?hl=%C1%E0%F0%EE%EC%E5%F2%F0.

6. В Україні в 2020 році зафіксували 1 мільйон кібератак – РНБО // MediaSapiens [Електронний ресурс]. – Режим доступу : https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvali-1-milion-kiberatak-rnbo/.

7. Бойко В.Д. Кібербезпека в країнах ЄС та країнах членах: генезис та проблеми її підвищення / В.Д. Бойко, М.Д. Василенко, С.В. Василенко [Електронний ресурс]. – Режим доступу : http://www.academy.ssu.gov.ua/ua/page/page_1581426437.htm.

References

1. Pro informatsiiu [Elektronnyi resurs] : Zakon Ukrainy vid 02.10.1992 № 2658-XII // Vidomosti Verkhovnoi Rady Ukrainy. – 1992. – № 48. – st. 651. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/2657-12#Text.

2. Sorokivska O.A. Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy / O.A. Sorokivska, V.L. Hevko // Herald of Khmelnytskyi National University. – 2010. – № 2. – T. 2. – S. 32–35.

3. Hoffman L.Dzh. Sovremennye metody zashity informacii / L. Dzh. Hoffman ; per. s angl. – M. : Sov. radio, 1980. – 57 s.

4. Novi vyklyky dlia informatsiinoi bezpeky pidpryiemstva: yak minimizuvaty potentsiini ryzyky [Elektronnyi resurs]. – Rezhym dostupu: https://eset.ua/ua/blog/view/67/novyye-vyzovy-dlya-informatsionnoy-bezopasnosti-predpriyatiya-kak-minimizirovat-potentsialnyye-riski.

5. Barometr riskov. Allianz nazval globalnye riski kompanij v 2018 godu // Forinshurer strahovanie [Elektronnyi resurs]. – Rezhym dostupu : https://forinsurer.com/news/18/01/26/35755?hl=%C1%E0%F0%EE%EC%E5%F2%F0.

6. V Ukraini v 2020 rotsi zafiksuvaly 1 milion kiberatak – RNBO // MediaSapiens [Elektronnyi resurs]. – Rezhym dostupu : https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvali-1-milion-kiberatak-rnbo/.

7. Boiko V.D. Kiberbezpeka v krainakh YeS ta krainakh chlenakh: henezys ta problemy yii pidvyshchennia / V.D. Boiko, M.D. Vasylenko, S.V. Vasylenko [Elektronnyi resurs]. – Rezhym dostupu : http://www.academy.ssu.gov.ua/ua/page/page_1581426437.htm.

Надійшла / Paper received: 19.08.2020 Надрукована / Paper Printed : 02-05.11.2020